UNIVERSIDAD CARLOS III DE MADRID
ESCUELA POLITÉCNICA SUPERIOR

INGENIERIA DE TELECOMUNICACIÓN
PROYECTO FIN DE CARRERA

PROTOCOLO AUTOORGANIZADO, SEGURO Y FIABLE PARA REDES DE SENSORES INALÁMBRICAS

(Resumen en castellano)

Autor: Celia de Dios Velasco

Tutor Universidad Aalborg (Dinamarca): Neeli R. Prasad

Tutor Universidad Carlos III de Madrid: Ana García Armada

Febrero 2009

Agradecimientos

Este proyecto está dedicado a mis padres y a mi hermana, que han estado apoyándome y ayudándome todos estos años para que siguiera estudiando, y que con este proyecto también finalizan una carrera.

También quiero dar las gracias a mis amigos de Getafe, a los del erasmus y a todos aquellos que durante estos años me han ofrecido su apoyo y amistad en los buenos y malos momentos.

1 Introducción

Este proyecto fin de carrera ha sido realizado en lengua inglesa en la universidad de Aalborg (Dinamarca) en el departamento de Sistemas Electrónicos, durante el segundo cuatrimestre del curso académico 2006-2007.

En este proyecto se propone un protocolo de seguridad con mecanismos de fiabilidad para ser utilizado en redes de sensores Wireless (WSNs) autoorganizadas. Este protocolo ha sido diseñado teniendo en cuenta las fuertes limitaciones que presentan los sensores actuales. También se ha evaluado el comportamiento del protocolo propuesto, para ello se implementó un simulador en lenguaje C que emulaba una red de sensores wireless funcionando con el protocolo propuesto.

Las redes de sensores inalámbricas están formadas por una gran cantidad de nodos sensores, éstos están distribuidos por diferentes lugares separados una cierta distancia para tomar medidas de variables del mundo real. En algunos casos los sensores se encuentran desplegados en áreas de difícil acceso por lo que el reemplazo de sus baterías no puede ser realizado de forma frecuente, éste hecho provoca que los nodos sensores sean dispositivos sobre los que se tenga que realizar un estricto control de su consumo de energía para alargar su tiempo de vida. El principal consumo de energía se produce cuando los nodos sensores se encuentran transmitiendo la información hacia otros nodos vecinos por lo que algoritmos centralizados no son recomendables en este tipo de aplicaciones. Por el contrario, algoritmos descentralizados donde la configuración de cada nodo depende exclusivamente de la información recogida por el mismo son muy aconsejables.

1.1 Motivación

Una de las principales motivaciones para la realización de este proyecto fue que en la actualidad existe una necesidad de monitorizar ambientes donde la seguridad y la fiabilidad en las comunicaciones es un requisito indispensable. Por ejemplo, en entornos médicos como hospitales donde el retraso en cualquier comunicación podría tener graves consecuencias. En estos casos es de vital importancia que los mensajes alcancen el nodo destino, es decir, fiabilidad en las comunicaciones.

Aunque existen diferentes protocolos de redes de sensores inalámbricas para aportar fiabilidad es todavía un desafío encontrar un protocolo que garantice seguridad y fiabilidad al mismo tiempo, debido a los limitados recursos que presentan los sensores. Por este motivo este proyecto fin de carrera se enfoca en encontrar un único protocolo autoorganizado que proporcione seguridad y fiabilidad en la comunicación entre sensores, optimizando en la medida de lo posible el consumo de energía de los sensores.

En lo que respecta a fiabilidad en este tipo de redes, se debe garantizar que el mayor número de paquetes enviados por la red alcancen el nodo destino. Con esto se evita consumir recursos mediante retransmisiones en capas superiores donde el tamaño del paquete es mayor.

El término en ingles Self-organization es muy utilizado en el contexto de redes de sensores inalámbricas, la traducción en castellano que se realizó fue autoorganización. Se puede definir como la capacidad que tiene toda la red de configurarse sin necesidad de depender de un nodo central. Se dice que una red de sensores es autoorgonizada cuando cada nodo sensor de la red puede configurarse mediante la información recogida desde sus vecinos y sin la existencia de un nodo central. La autoorganización mejora la escalabilidad de la red y provoca que sean necesarios menos mensajes de control. Por todo esto, el protocolo propuesto utiliza mecanismos distribuidos donde los nodos se puedan configurar ellos mismos con la información recibida desde sus vecinos sin depender de una estación central.
También existen problemas de interferencia en redes de sensores inalámbricas, puede existir solapamiento de redes y cada nodo debe ser capaz de identificar los sensores que pertenecen a su red para evitar gastar su limitada energía.

Este proyecto se centra en la seguridad dentro de la propia red y no se ocupa de la seguridad en la comunicación entre las diferentes redes de sensores inalámbricas.

2 Estado del arte

Para poder llevar a cabo este proyecto previamente se realizó un estudio sobre el estado del arte de la seguridad y fiabilidad en las redes de sensores inalámbricas, a continuación se resumen los principales conceptos tratados en la memoria.

2.1 Seguridad en redes de sensores inalámbricas

El medio inalámbrico es un medio inseguro por naturaleza, debido a que la información se transmite por el aire y cualquier intruso podría acceder a la información si ésta no es previamente protegida mediante algún mecanismo.

La seguridad en una red es un amplio concepto, en el caso de redes de sensores inalámbricas se centra en los siguientes requerimientos aunque esto siempre dependerá de la aplicación concreta donde se utilicen:

- AAA. Autorización, autenticación y accounting.
    - Autenticación Permite verificar al receptor que la información realmente ha sido enviada por el emisor que se identifica. Existen diferentes métodos de autenticación pero entre los mas utilizado en WSNs se encuentra el envío de una MAC (Message Authentication Code), funciones hash o intercambio de claves simétricas o asimétricas.
    - Autorización. El nodo debe tener los suficientes privilegios para poder acceder a los servicios de la red.
    - Accounting. Wikipedia define este concepto como el registro que se realiza del consumo que hacen los usuarios de los recursos de la red.
- Disponibilidad. Se debe garantizar que la red seguirá funcionando al introducir nuevos mecanismos para garantizar la seguridad en la comunicación.
- Seguridad semántica. Se pretende garantizar que todos los mensajes cifrados que circulan por la red sean siempre diferentes, incluso si el mismo mensaje se intentara cifrar varias veces. El inconveniente de esto es que normalmente se necesitan mecanismos de sincronización entre los nodos y más capacidades de almacenamiento para guardar las distintas claves para el cifrado.
- Frescura. Es necesario asegurar que antiguos mensajes no están circulando por la red para evitar el envío de ataques con mensajes de reply. Para solventar este

problema un identificador (“nonce”) o contador puede ser añadido dentro del paquete para asegurar la frescura del paquete recibido en el receptor. Algunos autores han identificado dos tipos de frescura (denominada en ingles “freshness”): débil cuando se proporciona orden parcial y no se preocupa del retraso en la información y fuerte cuando se proporciona orden total y se permite cierto retraso.

- Autoorganización (self-organization). En el contexto de redes de sensores inalámbricas siempre se debe usar mecanismos distribuidos para garantizar la escalabilidad de la red. Los nodos sensores deben formar una red de interconexión inalámbrica completamente autónoma y autoconfigurable.
- Confidencialidad. La información intercambiada entre dos nodos no puede ser entendida por un tercero. El principal mecanismo para proporcionar confidencialidad es la encriptación. Existen dos técnicas de cifrado dependiendo del algoritmo utilizado.
  - Algoritmos de clave simétrica. En este caso la misma clave es usada para encriptar y desencriptar. Su principal ventaja es que necesita enviar menos mensajes de control y no consume tanta potencia como los algoritmos asimétricos.
  - Algoritmos asimétricos. Estos sistemas usan un par de claves, una de ellas es utilizada para encriptar y la otra para desencriptar. Esta clase de sistemas son más lentos que los simétricos pero son más seguros.
- Integridad. Asegura que la información recibida no ha sido alterada durante la transmisión.

2.1.1 Protocolos de seguridad

Protocolos como IPSEC, SSL y SSH están funcionando adecuadamente en redes cableadas, sin embargo estos protocolos necesitan demasiados recursos para ser usados en redes de sensores inalámbricas.

En las redes de sensores inalámbricas se distinguen diferentes patrones de comunicación, los diferentes protocolos se centran en uno o en varios de éstos dependiendo de las aplicaciones para las que se orienten.

- Desde el nodo sensor a la estación base. Por ejemplo: lecturas de los sensores, alertas específicas.

- Desde la estación base al nodo sensor. Mensajes de intercambio de claves, peticiones especificas de la estación base, etc.
- Desde la estación base a todos los nodos. Mensajes de reprogramación de la red, etc.
- Comunicaciones entre nodos sensores.

En la siguiente tabla se muestra un cuadro resumen con los tres protocolos de seguridad más significativos en redes de sensores inalámbricas y los requerimientos que proporcionan cada uno de ellos:

Protocolo seguridad	**Patron de comunicación**	**Ventajas**	**Desventajas**
SNEP	Nodo → Sink Sink → Nodo Nodo → Nodo	Bajo overhead (8 bytes por mensaje) Proporciona: Seguridad semantic Autenticación Protección reply Débil frescura	Utiliza dos contadores para proporcionar seguridad semántica. Podrían aparecer problemas para sincronizar los contadores.
µTesla	Sink (Broadcast) → Nodo	Proporciona asimetría usando un mecanismo que envía las claves simétricas de revelación con cierto retraso No requiere muy estrecha sincronización entre nodo sensor y sink. Proporciona: Autenticado broadcast	No proporciona autenticación inmediata. El nodo receptor tiene que almacenar en su buffer los paquetes hasta que recibe la clave de revelación..
LEAP	Nodo→Sink Sink→Nodo Sink (broadcast) → Nodo Nodo→Nodo	Proporciona Autenticación Confidencialidad Robustez	Los nodos necesitan mas capacidades de almacenamiento, cada nodo sensor tiene que almacenar 4 tipos de claves Necesita de eficientes mecanismos para actualizar las claves. Considera que los nodos sensores no son móviles.

Protocolos de seguridad en redes de sensores inalámbricas

2.2 Fiabilidad en redes de sensores inalámbricas

Se puede definir la fiabilidad en redes de sensores inalámbricas como la capacidad de asegurar fiables transmisiones de datos en un estado de continuo cambio en la estructura de la red.

En lo que respecta a fiabilidad en este tipo de redes, se debe garantizar que el mayor número de paquetes enviados por la red alcancen el nodo destino. Con esto se evita consumir recursos mediante retransmisiones en capas superiores donde el tamaño del paquete es mayor.

En el caso de redes cableadas, el protocolo TCP es el principal ejemplo de protocolo fiable. Por el contrario, UDP se presenta como el protocolo no fiable en este tipo de redes.

Los dos mecanismos más comunes para proporcionar fiabilidad en WSNs son:

- Envío de paquetes NACKs ("Negative Acknowledmente"). Se envía este paquete para informar al emisor del número de paquetes perdidos que necesitan ser retransmitidos. El principal problema con este mecanismo surge en mensajes compuestos de muy pocos paquetes donde pueden perderse todos los paquetes.
- Envió de paquetes ACKs ("Acknowledmentent"). Con este mecanismo un mensaje ACK es esperado después de cada paquete enviado. El problema de éste surge en grandes redes donde el tráfico es elevado, el tráfico de control puede llegar a ser muy elevado con un gasto de energía demasiado alto que provoque la indisponibilidad de la red.

2.2.1 Protocolos de fiabilidad

En la actualidad existen diferentes protocolos para proporcionar fiabilidad a nivel de transporte en redes de sensores inalámbricas. Éstos se clasifican según el sentido de la comunicación, sink→nodos (descendente) o nodos →sink (ascendente). Y también se organizan dependiendo si el mecanismo trabaja salto a salto (entre nodos individuales) o end-to-end.

Los mecanismos end-to-end son recomendables en cuanto al consumo de energía en escenarios donde la probabilidad de perdida es baja, por el contrario mecanismos salto a salto consumen menos energía en entornos con alta probabilidad de perdida.

En el cuadro de abajo se resumen los principales protocolos para proporcionar fiabilidad en la comunicación de las redes de sensores inalámbricas.

	PSFQ	***RMST***	***ESRT***	***GARUDA***	***ART***
Fiabilidad	Descendente	Ascendente	Ascendente	Descendente	Ambos
	Sato a salto	Salto a salto / End to End	End to End	Salto a salto	End to End
Mecanismo	NACK	NACK	-	NACK	ACK/NACK
Preocupado por la energía	-	-	SI	-	SI
Recuperación de paquetes pérdidos	SI	SI	-	SI	SI

Protocolos de fiabiliad en redes de sensores inalámbricas

3 Propuesta de protocolo seguro y fiable distribuido

En este proyecto fin de carrera se propone un protocolo seguro y fiable de la capa de enlace para la comunicación entre los nodos sensores, éste esta basado en algunos de los mecanismos estudiados en las secciones 2.1.1 y 2.2.1.

Una de las principales características de este protocolo es que es completamente distribuido, no necesitara de ninguna estación central controlando el funcionamiento de los nodos. Debido a esto, los sensores pueden autoorganizarse ellos mismos con su información local.

Debido a las fuertes limitaciones que presentan los sensores en este protocolo se ha considerado muy importante la reutilización de variables y bloques funcionales con el objetivo de reducir el en la medida de lo posible el consumo de recursos y el tamaño del overhead del paquete, ya que se pretende que el protocolo sea realista y pueda ser implementado en el mayor número de sensores existentes en el mercado.

3.1 Requerimientos del protocolo

Los asuntos más importantes tratados en este protocolo son:

- Confidencialidad. Se proporciona mediante encriptado usando una clave secreta. Solo se utilizan mecanismos simétricos porque los asimétricos consumen demasiados recursos. Se propone el uso del algoritmo de encriptación Skipjack debido a su eficiencia de encriptación y a su bajo consumo de recursos.
- Autenticación, integridad y autorización. Se consigue mediante el uso de un código MAC en los paquetes, generado mediante encriptación reutilizando el bloque utilizado para proporcionar confidencialidad en los mensajes.
- Frescura. Este objetivo se proporciona incorporando un número de secuencia en los paquetes, de esta forma se evitan ataques de reply.
- Fiabilidad. Mediante el número de secuencia se identifica la pérdida de paquetes, se propone la utilización de mecanismos de NACKs con un cierto control de retransmisiones mediante un umbral para evitar llegar a consumir demasiada energía en los nodos sensores.
- Seguridad semántica. El número de secuencia se utiliza para cifrar el paquete de esta forma la salida del bloque cifrador siempre será diferente.

<table>
<tr><td colspan="5">Nodo-nodo. Protocolo de comunicación</td></tr>
<tr><td rowspan="2">Claves</td><td>K1</td><td colspan="2">Usado para computar el código MAC.</td><td rowspan="2">Globales constantes.</td></tr>
<tr><td>K2</td><td colspan="2">Usado junto con el numero de secuencia para encriptar los mensajes</td></tr>
<tr><td colspan="2" rowspan="2">Numero de secuencia</td><td colspan="2">Usado para proporcionar fiabilidad</td><td rowspan="2">Actualizadas como un contador con cada mensaje enviado</td></tr>
<tr><td colspan="2">Usado junto con K2 para encriptar los mensajes</td></tr>
<tr><td colspan="2" rowspan="2">Base de datos en cada nodo.</td><td colspan="3">Por cada vecino se mantendrá la siguiente información:</td></tr>
<tr><td>Identificador de vecino</td><td>Ultimo numero de secuencia recibido</td><td>Timestamp de la entrada</td></tr>
<tr><td colspan="2">Overhead:</td><td colspan="3">MAC code (8 Bytes) + Numero de secuencia (2 Bytes) = 10 extra Bytes por message</td></tr>
</table>

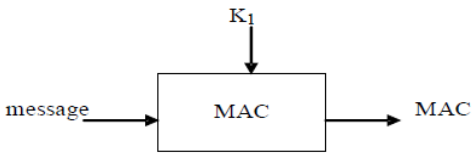
Resumen de las características del protocolo propuesto

3.2 Detalles del protocolo

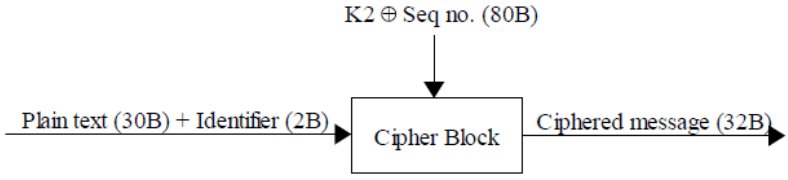
3.2.1 Envío de un paquete

Cuando un nodo quiera transmitir un mensaje, las siguientes acciones se llevaran a cabo:

- Generar el código MAC mediante la clave K1 (parámetro global de la red y conocido por todo los nodos)



- Cifrar el mensaje mediante un cifrador de bloque. Las dos entradas del cifrador serán: el mensaje y clave secreta. La clave secreta será construida mediante K2 y el número de secuencia del mensaje. K2 también es un parámetro global conocido por todos los nodos de la red.



No es necesario actualizar la clave K1 debido a que:

- El código MAC es más pequeño que el mensaje original. La salida no contiene toda la información del mensaje de entrada.
- El código MAC es generado con el mensaje sin encriptar por lo que un atacante necesitaría primero romper el algoritmo de encriptado para conocer que MAC corresponde con cada mensaje.

Finalmente, el mensaje enviado a la red tiene el siguiente formato:

Seq no.	MAC	Ciphered message
2 Bytes	8 Bytes	32 Bytes

El número de secuencia es enviado en claro para alcanzar una comunicación fiable y hacer posible la petición de retransmisión de los paquetes perdidos. Si el número de secuencia fuera enviado cifrado y el paquete se hubiera perdido, el receptor no sabría como descifrar correctamente el mensaje porque el mensaje se encuentra cifrado con la clave K2 y el número de secuencia.

3.2.2 Recepción de un paquete

En cada nodo receptor se debe mantener una tabla de vecinos, cada entrada tendrá tres campos con la siguiente información:

- Identificador de nodo vecino
- Ultimo número de secuencia recibido desde el vecino
- Timestamp para determinar cual es la entrada más antigua en la tabla.

Esta tabla será dinámica porque se ha supuesto que los nodos sensores vecinos no son siempre los mismos ya que los sensores podrían estar en movimiento y la calidad del enlace inalámbrico no siempre es constante.

Cuando un nodo recibe un paquete existen dos casos diferentes:

- El identificador de nodo recibido no se encuentra en la tabla de vecinos. El nodo receptor creará una entrada nueva en la tabla. (La tabla estará dimensionada con un número máximo de entradas y en caso de no haber ninguna libre se borrará la más antigua).
- El identificador de nodo recibido se encontraba ya registrado en la tabla de vecinos. En este caso si el número de secuencia recibido no es consecutivo con el almacenado existen tres posibilidades:

a) El protocolo detecta una diferencia pequeña entre el número de secuencia recibido y el número de secuencia almacenado, pide retransmisión de los paquetes perdidos.
b) Si la diferencia entre ambos números de secuencia supera un cierto umbral se decide no pedir por la retransmisión de los paquetes perdidos porque sería muy ineficiente. (Establecer previamente un umbral óptimo)
c) Se detecta que el número de secuencia recibido es menor que el almacenado para ese nodo en la tabla de vecinos. El paquete se descarta, podría estar siendo utilizado por un usuario mal intencionado para acceder a la red.

En el caso de que fuera necesario pedir por retransmisiones (caso a), el nodo receptor envía un mensaje NACK donde se incluye el ultimo número de secuencia recibido correctamente y el identificador del nodo que debe enviar de nuevo esos paquetes que se perdieron en la red.

4 Conclusiones

Las redes de sensores inalámbricas presentan muchos problemas para proporcionar seguridad y fiabilidad debido a sus limitados recursos (memoria, capacidad de proceso, limitada potencia) y a las características del canal inalámbrico. La necesidad de ambos requisitos depende de la aplicación donde se enfoquen dichas redes.

Existen aplicaciones donde la fiabilidad no se presenta como un requisito indispensable debido a que la pérdida de un paquete no supone graves consecuencias, este es el caso de aplicaciones de medida de temperatura. Sin embargo existen aplicaciones utilizadas en situaciones de emergencia donde es muy importante que la información captada por los nodos sensores alcance el nodo destino. Los protocolos existentes en las redes convencionales necesitan demasiados recursos de los dispositivos sensores para ser utilizados en este contexto.

El protocolo propuesto ha tenido en consideración los siguientes aspectos: integridad, autenticación, autorización, autoorganización, seguridad semántica, frescura y fiabilidad. Teniendo en cuenta la limitación de recursos que presentan los sensores en dichas redes.

El funcionamiento del protocolo fue evaluado mediante un simulador realizado en C durante el desarrollo de este proyecto. En los resultados de dicha simulación, se ha comprobado que podría ser implementado sobre los sensores que existen actualmente en el mercado como podría ser el Mica2. También se observa como la incorporación de mecanismos que proporcionan fiabilidad y seguridad en la red suponen un incremento en el consumo de energía de los sensores, este hecho debe ser tenido en cuenta si se pretende utilizar dicho protocolo en entornos donde el reemplazo de los sensores no es de fácil acceso.

En comparación con otros protocolos existentes se puede concluir que el protocolo propuesto añade menos overhead que el protocolo de seguridad SNEP pero sin embargo consume más energía debido a las retransmisiones.

Se propone la utilización del protocolo diseñado en entornos médicos, escenario en el cual la fiabilidad en las comunicaciones es indispensable y el gasto de energía extra podría ser justificado por la necesidad de fiabilidad.

Se puede encontrar más información sobre el protocolo propuesto y su correspondiente simulación en la memoria realizada en ingles que se encuentra almacenada dentro de este mismo CD.

5 Trabajo futuro

Mediante este proyecto se ha propuesto un nuevo protocolo seguro y fiable para las comunicaciones en las redes de sensores inalámbricas, se realizo su simulación demostrando que podría ser implementado sobre sensores reales. El siguiente paso sería su implementación sobre sensores reales para comprobar su funcionamiento y poder comparar los resultados.
Las simulaciones fueron realizadas con un modelo de canal shadowing log-normal. Otros modelos podrían ser incluidos añadiendo más propiedades del canal inalámbrico.

También se asumió que las claves secretas usadas para el proceso de encriptación eran conocidas a priori por todos los nodos de la red. La solución sería más flexible si previamente se estudiará la distribución segura de dichas claves.

Sobre el protocolo propuesto se podrían incluir nuevas técnicas como las usadas en PSFQ para proporcionar mayor fiabilidad en las comunicaciones cuando los mensajes son pequeños.